

Seguridad en iOS y Android: un Análisis Comparativo

Tesina de Grado

Licenciatura en Ciencias de la Computación

Autor:

Raúl Ignacio Galuppo

Director:

Dr. Carlos Luna

28 de marzo de 2018

1 Introducción

- Motivación
- Modelo de Android
- Modelo de iOS

1 Introducción

- Motivación
- Modelo de Android
- Modelo de iOS

2 Análisis Comparativo

1 Introducción

- Motivación
- Modelo de Android
- Modelo de iOS

2 Análisis Comparativo

3 Hacia un Framework para la Comparación de Permisos

1 Introducción

- Motivación
- Modelo de Android
- Modelo de iOS

2 Análisis Comparativo

3 Hacia un Framework para la Comparación de Permisos

4 Conclusiones y Trabajos Futuros

Motivación

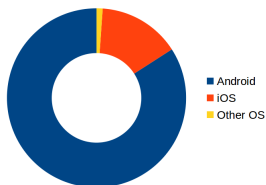


Figura 1 : Ventas mundiales de teléfonos inteligentes a usuarios finales por so.

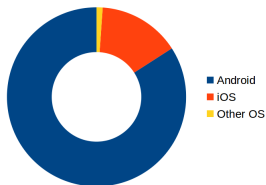


Figura 1 : Ventas mundiales de teléfonos inteligentes a usuarios finales por so.

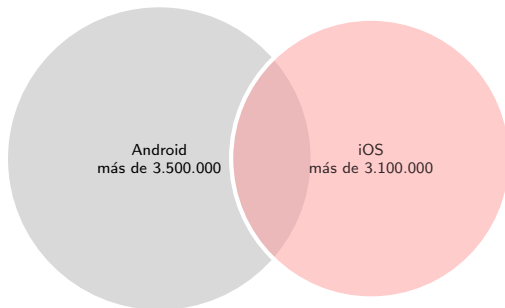


Figura 2 : Cantidad de aplicaciones móviles.

Motivación I

Se incrementan los ataques a los dispositivos móviles, en busca de información personal y confidencial que almacenan, y de las operaciones realizadas a través de ellos.

Motivación I

Se incrementan los ataques a los dispositivos móviles, en busca de información personal y confidencial que almacenan, y de las operaciones realizadas a través de ellos.

Motivación II

Debido al uso diario de estas aplicaciones, se puede filtrar una gran cantidad de información privada y confidencial.

Modelo de Android

Modelo de Android

- Android es un sistema operativo de código abierto, diseñado para dispositivos móviles y desarrollado por Google junto con la Open Handset Alliance.

Modelo de Android

- Android es un sistema operativo de código abierto, diseñado para dispositivos móviles y desarrollado por Google junto con la Open Handset Alliance.

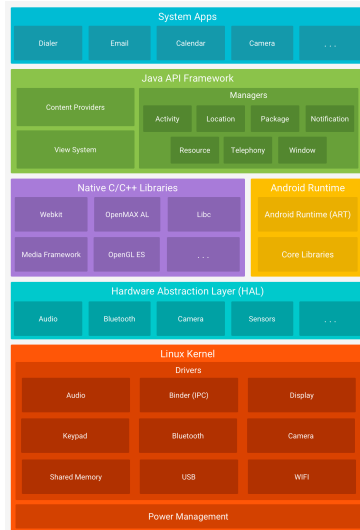


Figura 3 : Capas de Android.

Modelo de Android

- Android es un sistema operativo de código abierto, diseñado para dispositivos móviles y desarrollado por Google junto con la Open Handset Alliance.
- Cada aplicación corre en un *entorno aislado*, forzando a que solo pueda tener acceso a sus recursos.

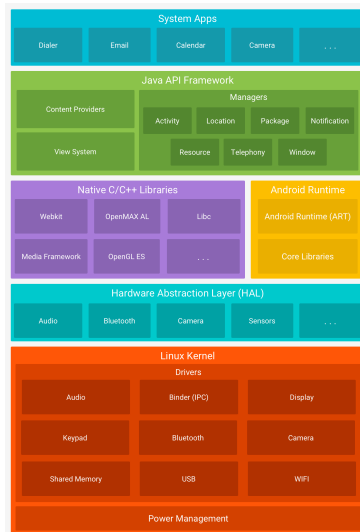


Figura 3 : Capas de Android.

Modelo de Android

- Podemos clasificar los permisos según el riesgo implícito al otorgarlos:
 - *Normal*

Modelo de Android

- Podemos clasificar los permisos según el riesgo implícito al otorgarlos:
 - *Normal*
 - *Dangerous*

Modelo de Android

- Podemos clasificar los permisos según el riesgo implícito al otorgarlos:
 - *Normal*
 - *Dangerous*
 - *Signature*

Modelo de Android

- Podemos clasificar los permisos según el riesgo implícito al otorgarlos:
 - *Normal*
 - *Dangerous*
 - *Signature*
 - *Signature/System*

Modelo de Android

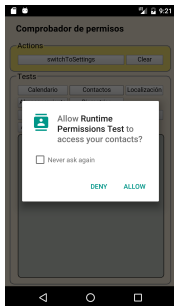
- Podemos clasificar los permisos según el riesgo implícito al otorgarlos:
 - **Normal**
 - **Dangerous**

Modelo de Android

- Podemos clasificar los permisos según el riesgo implícito al otorgarlos:
 - **Normal**
 - **Dangerous**
- A partir de la versión 6.0 se propone un nuevo modelo de permisos:

Modelo de Android

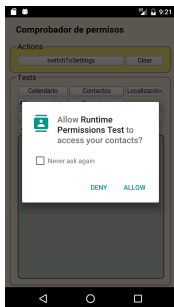
- Podemos clasificar los permisos según el riesgo implícito al otorgarlos:
 - **Normal**
 - **Dangerous**
- A partir de la versión 6.0 se propone un nuevo modelo de permisos:



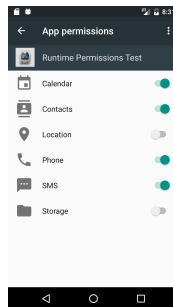
(a) Solicitud de un permiso.

Modelo de Android

- Podemos clasificar los permisos según el riesgo implícito al otorgarlos:
 - **Normal**
 - **Dangerous**
- A partir de la versión 6.0 se propone un nuevo modelo de permisos:



(a) Solicitud de un permiso.



(b) Listado de los permisos.

Figura 4 : Nuevo modelo de permisos.

Modelo de iOS

- iOS es un sistema operativo para dispositivos móviles de la multinacional Apple Inc. diseñado para ser seguro.

Modelo de iOS

- iOS es un sistema operativo para dispositivos móviles de la multinacional Apple Inc. diseñado para ser seguro.
- Las principales características de seguridad no son configurables y vienen habilitadas por defecto.

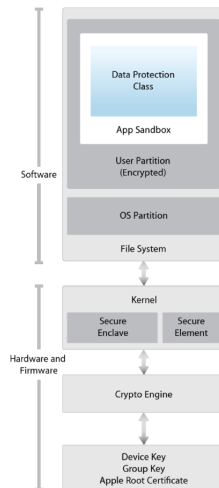


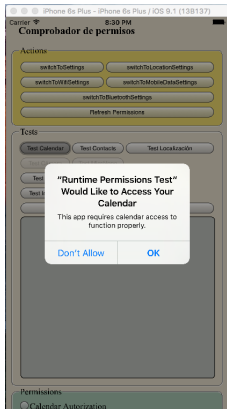
Figura 5 : Entorno seguro de iOS.

Modelo de iOS

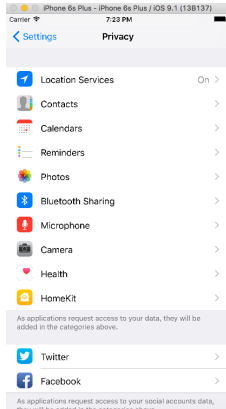
- Las aplicaciones pueden solicitar un permiso solamente mientras se esté ejecutando.

Modelo de iOS

- Las aplicaciones pueden solicitar un permiso solamente mientras se esté ejecutando.



(a) Solicitud de un permiso.



(b) Control de privacidad.

Figura 6 : Sistema de permisos de iOS 9.

Análisis Comparativo

- Existen muchos trabajos sobre distintas formas de comparar la seguridad de ambas plataformas.

- Existen muchos trabajos sobre distintas formas de comparar la seguridad de ambas plataformas.
- Esta tesina propone analizar distintas características relacionadas a la privacidad del usuario,

- Existen muchos trabajos sobre distintas formas de comparar la seguridad de ambas plataformas.
- Esta tesina propone analizar distintas características relacionadas a la privacidad del usuario, poniendo foco en *los permisos que se pueden modificar en tiempo de ejecución*.

- Existen muchos trabajos sobre distintas formas de comparar la seguridad de ambas plataformas.
- Esta tesina propone analizar distintas características relacionadas a la privacidad del usuario, poniendo foco en *los permisos que se pueden modificar en tiempo de ejecución*.
- Se analizaron cinco características presentes en iOS y Android:

- Existen muchos trabajos sobre distintas formas de comparar la seguridad de ambas plataformas.
- Esta tesina propone analizar distintas características relacionadas a la privacidad del usuario, poniendo foco en *los permisos que se pueden modificar en tiempo de ejecución*.
- Se analizaron cinco características presentes en iOS y Android:
 - Arranque verificado

- Existen muchos trabajos sobre distintas formas de comparar la seguridad de ambas plataformas.
- Esta tesina propone analizar distintas características relacionadas a la privacidad del usuario, poniendo foco en *los permisos que se pueden modificar en tiempo de ejecución*.
- Se analizaron cinco características presentes en iOS y Android:
 - Arranque verificado
 - Cifrado del sistema de archivos

- Existen muchos trabajos sobre distintas formas de comparar la seguridad de ambas plataformas.
- Esta tesina propone analizar distintas características relacionadas a la privacidad del usuario, poniendo foco en *los permisos que se pueden modificar en tiempo de ejecución*.
- Se analizaron cinco características presentes en iOS y Android:
 - Arranque verificado
 - Cifrado del sistema de archivos
 - Bloqueo del dispositivo

- Existen muchos trabajos sobre distintas formas de comparar la seguridad de ambas plataformas.
- Esta tesina propone analizar distintas características relacionadas a la privacidad del usuario, poniendo foco en *los permisos que se pueden modificar en tiempo de ejecución*.
- Se analizaron cinco características presentes en iOS y Android:
 - Arranque verificado
 - Cifrado del sistema de archivos
 - Bloqueo del dispositivo
 - Seguridad de las aplicaciones

- Existen muchos trabajos sobre distintas formas de comparar la seguridad de ambas plataformas.
- Esta tesina propone analizar distintas características relacionadas a la privacidad del usuario, poniendo foco en *los permisos que se pueden modificar en tiempo de ejecución*.
- Se analizaron cinco características presentes en iOS y Android:
 - Arranque verificado
 - Cifrado del sistema de archivos
 - Bloqueo del dispositivo
 - Seguridad de las aplicaciones
 - **Sistema de permisos**

Al comparar la gestión de permisos de ambas plataformas, encontramos varias similitudes:

Al comparar la gestión de permisos de ambas plataformas, encontramos varias similitudes:

- A una aplicación se le otorga permisos básicos al momento de instalación, sin posibilidad de revocarlos.

Al comparar la gestión de permisos de ambas plataformas, encontramos varias similitudes:

- A una aplicación se le otorga permisos básicos al momento de instalación, sin posibilidad de revocarlos.
- Si una aplicación necesita un permiso no básico, debe requerirlo. El usuario puede otorgarlo o revocarlo.

Análisis Comparativo

Respecto a cómo se definen los permisos:

Análisis Comparativo

Respecto a cómo se definen los permisos:

- En Android están orientados según el riesgo implícito al otorgarlos.

Análisis Comparativo

Respecto a cómo se definen los permisos:

- En Android están orientados según el riesgo implícito al otorgarlos.
- En iOS los permisos están orientados a los componentes.

Análisis Comparativo

Respecto a cómo se definen los permisos:

- En Android están orientados según el riesgo implícito al otorgarlos.
- En iOS los permisos están orientados a los componentes.

Medida de comparación: *dos permisos son similares si resguardan un componente que provee la misma funcionalidad.*

Análisis Comparativo

Respecto a cómo se definen los permisos:

- En Android están orientados según el riesgo implícito al otorgarlos.
- En iOS los permisos están orientados a los componentes.

Medida de comparación: *dos permisos son similares si resguardan un componente que provee la misma funcionalidad.*

Ambas plataformas	Permisos	
	Solo en Android	Solo en iOS
Calendario	-	-
Contactos	-	-
Cámara	-	-
Localización	-	-
-	-	Compartir por Bluetooth
Microfono	-	-
-	Teléfono	-
Sensores	-	-
-	SMS	-
-	Almacenamiento	-
-	-	Homekit
-	-	Redes Sociales
-	-	Diagnóstico
-	-	Publicidad

Cuadro 1 : Resultado de la comparación de permisos.

Respecto del alcance del sistema de permisos:

Respecto del alcance del sistema de permisos:

- En Android, un permiso es a nivel de grupo. Por lo tanto, el usuario otorga o deniega para todo el grupo.

Respecto del alcance del sistema de permisos:

- En Android, un permiso es a nivel de grupo. Por lo tanto, el usuario otorga o deniega para todo el grupo.
- La misma situación ocurre en iOS: se otorga un permiso de acceso a todas las funcionalidades de un determinado componente.

Si observamos la cobertura del sistema de permisos,

Si observamos la cobertura del sistema de permisos, las dos plataformas dejan funcionalidades sin permisos modificables *en tiempo de ejecución*:

Si observamos la cobertura del sistema de permisos, las dos plataformas dejan funcionalidades sin permisos modificables *en tiempo de ejecución*:

- En Android se destacan: Acceso a Internet, Compartir vía Bluetooth e Información del Dispositivo.

Si observamos la cobertura del sistema de permisos, las dos plataformas dejan funcionalidades sin permisos modificables *en tiempo de ejecución*:

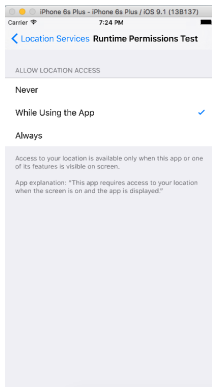
- En Android se destacan: Acceso a Internet, Compartir vía Bluetooth e Información del Dispositivo.
- En iOS se destacan: Acceso a Internet y SMS. Tampoco tiene la suficiente granularidad para administrar el acceso a los datos de las llamadas telefónicas.

Análisis Comparativo

Para finalizar se analiza la interacción con el usuario:

Análisis Comparativo

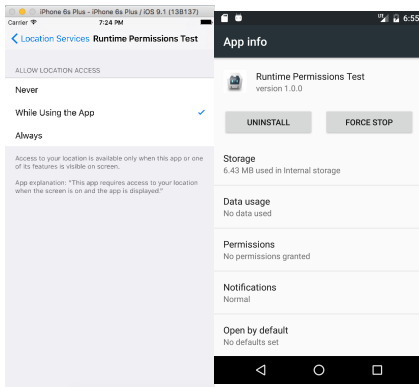
Para finalizar se analiza la interacción con el usuario:



(a) Permisos
requeridos por una
aplicación.

Análisis Comparativo

Para finalizar se analiza la interacción con el usuario:

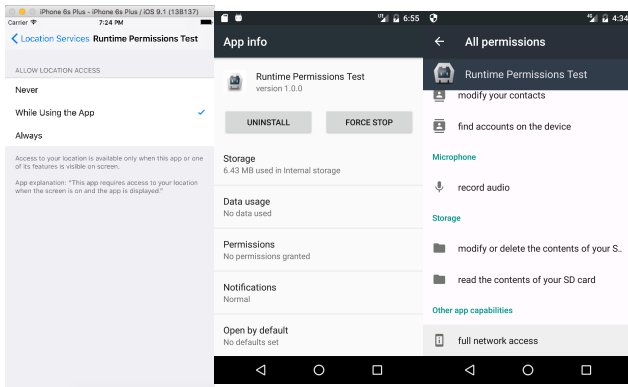


(a) Permisos
requeridos por una
aplicación.

(b) La aplicación
no tiene ningún
permiso.

Análisis Comparativo

Para finalizar se analiza la interacción con el usuario:



(a) Permisos requeridos por una aplicación.

(b) La aplicación no tiene ningún permiso.

(c) Tiene todos los permisos *normales*.

Figura 7 : Interacción con el usuario en iOS y Android.

Framework para la Comparación de Permisos

Hacia un Framework para la Comparación de Permisos

Se ha desarrollado un *framework* para determinar empíricamente el alcance de los sistemas de permisos de ambas plataformas.

Hacia un Framework para la Comparación de Permisos

Se ha desarrollado un *framework* para determinar empíricamente el alcance de los sistemas de permisos de ambas plataformas.

Objetivo I

Se busca dejar en evidencia posibles vulnerabilidades presentes en los modelos de seguridad.

Hacia un Framework para la Comparación de Permisos

Se ha desarrollado un *framework* para determinar empíricamente el alcance de los sistemas de permisos de ambas plataformas.

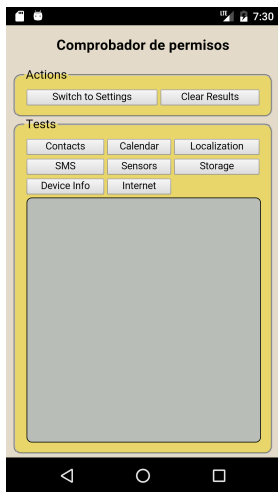
Objetivo I

Se busca dejar en evidencia posibles vulnerabilidades presentes en los modelos de seguridad.

Objetivo II

Se intenta averiguar cuál es la cobertura del sistema de permisos respecto de los datos sensibles para la privacidad.

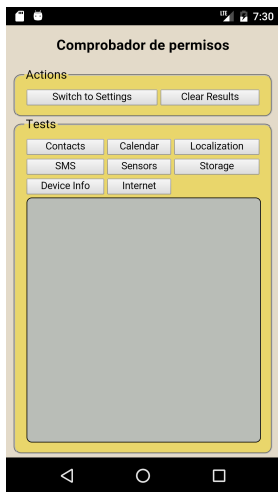
Hacia un Framework para la Comparación de Permisos



El *framework* es una aplicación móvil híbrida desarrollada con Apache Cordova

Figura 8 : Áreas del *framework*.

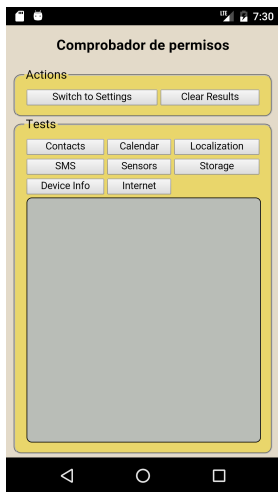
Hacia un Framework para la Comparación de Permisos



El *framework* es una aplicación móvil híbrida desarrollada con Apache Cordova y está compuesto por varios tests.

Figura 8 : Áreas del *framework*.

Hacia un Framework para la Comparación de Permisos



El *framework* es una aplicación móvil híbrida desarrollada con Apache Cordova y está compuesto por varios tests.

Se utilizaron los emuladores oficiales para testear el *framework* propuesto.

Figura 8 : Áreas del *framework*.

Hacia un Framework para la Comparación de Permisos

Utilizando *framework* se pueden testear:

- Contactos
- Calendario
- Geolocalización
- SMS
- Sensores
- Almacenamiento
- Información del dispositivo
- Acceso a Internet

Hacia un Framework para la Comparación de Permisos

Utilizando *framework* se pueden testear:

- Contactos
- Calendario
- Geolocalización
- SMS
- Sensores
- Almacenamiento
- Información del dispositivo
- Acceso a Internet

Sin embargo, no se pueden testear:

- WIFI
- Bluetooth
- NFC
- Conexiones USB
- Micrófono
- Cámara

Hacia un Framework para la Comparación de Permisos

Por ejemplo:



(a) Mensaje de Error. (b) Mensaje exitoso.

c Test de Contactos

- 1: Se imprimen por consola todos los contactos.
- 2: Se crea un nuevo contacto.
- 3: Se vuelven a imprimir por consola todos los contactos.

Permisos: [Contacto](#), tanto para Android como para iOS.

Plugin: `cordova-plugin-contacts(v. 2.3.1).`

Hacia un Framework para la Comparación de Permisos

Permisos			
<i>Clase A</i>	<i>Clase B</i>	<i>Clase C</i>	<i>Clase D</i>
Contactos	-	-	-
Calendario	-	-	-
Geolocalización	-	-	-
-	SMS	-	-
-	Almacenamiento	-	-
-	-	-	Sensores
-	-	-	Información del dispositivo
-	-	-	Acceso a Internet

Cuadro 2 : Clasificación de componentes.

Hacia un Framework para la Comparación de Permisos

Permisos			
Clase A	Clase B	Clase C	Clase D
Contactos	-	-	-
Calendario	-	-	-
Geolocalización	-	-	-
-	SMS	-	-
-	Almacenamiento	-	-
-	-	-	Sensores
-	-	-	Información del dispositivo
-	-	-	Acceso a Internet

Cuadro 2 : Clasificación de componentes.

Criterio: requieren autorización explícita del usuario para utilizarlos.

Conclusiones y Trabajos Futuros

Primer Aporte

Un análisis comparativo entre algunas características presentes en los modelos de seguridad de ambas plataformas.

Primer Aporte

Un análisis comparativo entre algunas características presentes en los modelos de seguridad de ambas plataformas.

Segundo Aporte

Se logró establecer una clasificación de todos los permisos que un usuario puede cambiar en tiempo de ejecución.

Medida de comparación: *dos permisos son similares si resguardan un componente que provee la misma funcionalidad.*

Conclusiones

Primer Aporte

Un análisis comparativo entre algunas características presentes en los modelos de seguridad de ambas plataformas.

Segundo Aporte

Se logró establecer una clasificación de todos los permisos que un usuario puede cambiar en tiempo de ejecución.

Medida de comparación: *dos permisos son similares si resguardan un componente que provee la misma funcionalidad.*

Tercer Aporte

El *Framework para la Comparación de Permisos* multiplataforma.

Conclusiones

Primer Aporte

Un análisis comparativo entre algunas características presentes en los modelos de seguridad de ambas plataformas.

Segundo Aporte

Se logró establecer una clasificación de todos los permisos que un usuario puede cambiar en tiempo de ejecución.

Medida de comparación: *dos permisos son similares si resguardan un componente que provee la misma funcionalidad.*

Tercer Aporte

El *Framework para la Comparación de Permisos* multiplataforma.

Cuarto Aporte

Se determinó una clasificación de componentes.

Criterio: *un componente pertenece a una clase según requiera autorización explícita del usuario para utilizarlo.*

Trabajos futuros

Para finalizar, se enumeran algunas líneas a seguir como trabajos a futuro:

Trabajos futuros

Para finalizar, se enumeran algunas líneas a seguir como trabajos a futuro:

- Probar y mejorar los tests en dispositivos reales.

Trabajos futuros

Para finalizar, se enumeran algunas líneas a seguir como trabajos a futuro:

- Probar y mejorar los tests en dispositivos reales.
- Desarrollar tests para las funcionalidades que no pueden ser emuladas.

Trabajos futuros

Para finalizar, se enumeran algunas líneas a seguir como trabajos a futuro:

- Probar y mejorar los tests en dispositivos reales.
- Desarrollar tests para las funcionalidades que no pueden ser emuladas.
- Desarrollar un test para poder comparar el cifrado de archivos.

Trabajos futuros

Para finalizar, se enumeran algunas líneas a seguir como trabajos a futuro:

- Probar y mejorar los tests en dispositivos reales.
- Desarrollar tests para las funcionalidades que no pueden ser emuladas.
- Desarrollar un test para poder comparar el cifrado de archivos.
- No sabemos qué permisos básicos otorga iOS. Se podrían desarrollar varios tests para descubrirlos.

Para finalizar, se enumeran algunas líneas a seguir como trabajos a futuro:

- Probar y mejorar los tests en dispositivos reales.
- Desarrollar tests para las funcionalidades que no pueden ser emuladas.
- Desarrollar un test para poder comparar el cifrado de archivos.
- No sabemos qué permisos básicos otorga iOS. Se podrían desarrollar varios tests para descubrirlos.
- En el informe se mencionan algunos análisis previos relacionados a la seguridad de Android y/o de iOS. Se podría profundizar más en comparar el modelo propuesto en el presente informe con los análisis mencionados previamente.

Para finalizar, se enumeran algunas líneas a seguir como trabajos a futuro:

- Probar y mejorar los tests en dispositivos reales.
- Desarrollar tests para las funcionalidades que no pueden ser emuladas.
- Desarrollar un test para poder comparar el cifrado de archivos.
- No sabemos qué permisos básicos otorga iOS. Se podrían desarrollar varios tests para descubrirlos.
- En el informe se mencionan algunos análisis previos relacionados a la seguridad de Android y/o de iOS. Se podría profundizar más en comparar el modelo propuesto en el presente informe con los análisis mencionados previamente.
- Dado que salieron al mercado Android 8.0 e iOS 11, se podría analizar extender el *framework* para las características de seguridad adicionales en dichas versiones.

¿ Preguntas ?





¡¡ Mil gracias por venir !!